



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/027,780	12/20/2001	Eyal Cohen	135.001US01	9593
7590	11/17/2006			
			EXAMINER	
			WILLIAMS, JEFFERY L	
			ART UNIT	PAPER NUMBER
			2137	

Mark M. Friedman
Dr. Mark Friedman Ltd.
c/o Polkinghorn
9003 Florin way
Upper Marlboro, MD 20772

DATE MAILED: 11/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/027,780	COHEN, EYAL	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 18 August 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 18-37 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 18-37 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 29 November 2005 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____

Art Unit: 2137

1 **DETAILED ACTION**

2

3 This action is in response to the communication filed on 8/18/06.

4 All objections and rejections not set forth below have been withdrawn.

5

6 ***Continued Examination Under 37 CFR 1.114***

7

8 A request for continued examination under 37 CFR 1.114, including the fee set
9 forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this
10 application is eligible for continued examination under 37 CFR 1.114, and the fee set
11 forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action
12 has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/18/06
13 has been entered.

14

15

16 ***Claim Rejections - 35 USC § 102***

17

18 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that
19 form the basis for the rejections under this section made in this Office action:

20 A person shall be entitled to a patent unless –

21 (e) the invention was described in (1) an application for patent, published under section 122(b), by
22 another filed in the United States before the invention by the applicant for patent or (2) a patent
23 granted on an application for patent by another filed in the United States before the invention by the
24 applicant for patent, except that an international application filed under the treaty defined in section
25 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

Art Unit: 2137

1 only if the international application designated the United States and was published under Article 21(2)
2 of such treaty in the English language.

3
4 **Claims 18 – 37 are rejected under 35 U.S.C. 102(e) as being anticipated by**

5 **Candelore et al., (Candelore), “Secure Processor With External Memory Using**

6 **Block Chaining and Block Re-Ordering”, U.S. Patent 6,061,449.**

7
8 Regarding claim 18, Candelore discloses:

9 (a) *designating a plurality of critical locations within the executable program file*

10 (28:27-38 – Candelore discloses the designation of locations within the file to be

11 modified for the protection scheme); (b) *arming the executable program file, thereby*

12 *producing a modified executable program file by including a plurality of software*

13 *procedures at said locations wherein each said software procedure performs at least*

14 *one linked portion of the securing* (25:20-28, 50-58 – Candelore discloses the “arming”

15 of the file by producing a modified executable file, wherein the file includes modified

16 software procedures at the designated locations to perform “linked” “securing”); (c)

17 *storing said modified executable program file in storage operatively attached to a*

18 *computer (fig. 1, elem. 110); and (d) executing in a computer said modified executable*

19 *program file, thereby running said software procedures solely upon reaching said*

20 *respective locations* (28:8-18).

21
22 Regarding claim 19, Candelore discloses:

23 *wherein the securing includes using a key from at least one of said software*

24 *procedures to decrypt at least one other of said software procedures* (15:30-46).

1

2 Regarding claim 20, Candelore discloses:

3 *wherein said executing includes self-decrypting said modified executable*

4 *program file and secured digital content accessible by said executable program file*

5 (15:28-45 – Candelore discloses a method for executing, wherein the method includes

6 decrypting (“self-decrypting”, as the method for decrypting is part of the execution

7 method itself) the program file and secure content).

8

9 Regarding claim 21, Candelore discloses:

10 *wherein said arming includes storing in at least one of said software procedures*

11 *at least a reference to a key, wherein said key is required for accessing another of said*

12 *software procedures* (20:5-35).

13

14 Regarding claim 22, Candelore discloses:

15 *wherein said designating is performed by an owner of digital content accessible*

16 *by said executable program file* (28:27-38).

17

18 Regarding claim 23, Candelore discloses:

19 (e) *verifying an authentication key accessible over the internet* (11:36-51 – an

20 arrangement of bits, such as a key, is inherently able to be obtained from a medium,

21 such as the Internet. The descriptive language, being “accessible” or “able to be

22 accessed”, clearly is applicable to any arrangement of bits, as bits can be transmitted

Art Unit: 2137

1 and received over the Internet. Furthermore, describing bits as capable of being
2 transmitted does not further limit structure and require that bits be transmitted).

3

4 Regarding claim 24, Candelore discloses:

5 *(e) upon said executing, accessing secured digital content stored on a digital*
6 *medium, wherein at least one key required for said accessing is stored on said digital*
7 *medium* (15:42-47 – the key and the secure digital content are found to be co-located
8 within the same medium).

9

10 Regarding claim 25, Candelore discloses:

11 *wherein said at least one key is required to decrypt said secured digital content*
12 (15:42-47).

13

14 Regarding claim 26, Candelore discloses:

15 *wherein said at least one key is stored on said digital medium* (15:42-47 – the
16 key is both an “authentication key” (as the correct key will only decrypt the correct
17 content, thus indicating is the correct/authentic content was received) and a content key
18 (as it decrypts the content). The key and the secure digital content are found to be co-
19 located within the same medium).

20

21 Regarding claim 27, Candelore discloses:

Art Unit: 2137

1 *wherein said at least one key has at least one address stored solely in at least*

2 *one of said software procedures* (15:42-47 - The key's address, location of storage, is

3 derived from the "at least one of said software procedures").

4

5 Regarding claim 28, Candelore discloses:

6 *wherein said at least one key is provided by an address conversion module*

7 *stored on said digital medium* (15:42-47 – The key is found to be used by the system of

8 Candelore, thus the system inherently includes a module to find the location of the key).

9

10 Regarding claim 29, Candelore discloses:

11 *wherein at least one of said software procedures is encrypted using at least one*

12 key (25:20-28, 50-58; 28:8-18).

13

14 Regarding claim 30, Candelore discloses:

15 *wherein at least one of said software procedures receives at least a portion of a*

16 key from at least one other of said software procedures (25:20-28, 50-58; 28:8-18).

17

18 Regarding claim 31, Candelore discloses:

19 *wherein a key is determined by selectively either a specific location within said*

20 software procedure or a calculation based on the software procedure, further

21 comprising the step of: (d) accessing another said software procedure using said key

22 (25:20-28, 50-58; 28:8-18).

Art Unit: 2137

1
2 Regarding claim 32, Candelore discloses:
3 *wherein said software procedures are concealed within the executable program*
4 *file* (26:14-24).

5
6 Regarding claim 33, Candelore discloses:
7 *wherein said designating includes introducing flags within said executable*
8 *program file, wherein said flags designate said critical locations within said executable*
9 *program file* (28:27-38 – Candelore discloses that the program is divided into defined
10 structural boundaries, the boundaries indicating the location of secured blocks).

11
12 Regarding claim 34, Candelore discloses:
13 *wherein portions of said executable program file are occluded by said software*
14 *procedures* (25:20-28, 50-58; 28:8-18, 27-38).

15
16 Regarding claim 35, Candelore discloses:
17 *A digital storage medium including the modified executable program file*
18 *produced according to the method of claim 18* (fig. 1).

19
20 Regarding claim 36, Candelore discloses:
21 *A digital storage medium storing secured digital content accessible by a modified*
22 *executable program file produced according to the method of claim 18* (fig. 1).

Art Unit: 2137

1
2 Regarding claim 37, it is the computer medium and instructions claim
3 corresponding the method claim 18, and it is rejected, at least, for the same reasons.

Response to Arguments

Applicant's arguments filed 8/18/06 have been fully considered but they are not persuasive.

Applicants argue primarily that:

12

13 (i) *Applicant has very carefully reviewed Candelore, and has not found any*

14 *reference or suggestion to steps of the present invention: designating a critical locations*

15 *within the executable program file; and arming the executable program file, by including*

16 *software procedures or mines at the locations. ... Candelore is simply pointing out ...*

17 (Remarks, pg. 8)

19 In response, the examiner respectfully notes that Applicant's arguments fail to
20 comply with 37 CFR 1.111(b) because they amount to a general allegation that the
21 claims define a patentable invention without specifically pointing out how the language
22 of the claims patentably distinguishes them from the references.

1
2 (ii) *Applicant respectfully submits that neither Candelore nor Lie nor any other*
3 *reference in the field of secure processors and cipher block chaining teaches, suggests*
4 *or implies designating a critical locations within the executable program file; and arming*
5 *the executable program file, by including software procedures or mines at the locations.*
6 *In cipher block chaining, each data file of for instance 80,000 bytes is divided*
7 *automatically into 10,000 blocks, each block of 8 bytes. Hence, in cipher block chaining*
8 *there is no step analogous to designation of critical locations within the data. (Remarks,*
9 *pg. 8,9)*

10
11 In response, the examiner respectfully points out that the applied prior art is
12 Candelore, thus any arguments against Lie or other unapplied references are not
13 persuasive.

14 Furthermore, the examiner points out that the applicant essentially argues that
15 the prior art does not disclose the designation of critical locations since the prior art is
16 alleged to perform in an automated fashion. In response, the examiner asserts that
17 regardless of if prior art discloses the claimed limitations as being performed
18 automatically or as performed non-automatically, the prior art still discloses the claimed
19 limitations.

20
21 (iii) *Hence, in cipher block chaining there is no step analogous to designation of*
22 *critical locations within the data. In cipher block chaining, there is no designation of*

1 *critical locations in the program file and/or digital content to be encrypted. In fact,*
2 *disclosures in the field of "cipher block chaining" teach away from the present invention.*
3 *In cipher block chaining, the division into blocks is performed blindly and uniformly*
4 *without considering the criticality of the locations within the data to be encrypted.*

5 (Remarks, pg. 9)

6

7 Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount
8 to a general allegation that the claims define a patentable invention without specifically
9 pointing out how the language of the claims patentably distinguishes them from the
10 references.

11 Furthermore, in response to applicant's argument that the references fail to show
12 certain features of applicant's invention, it is noted that the features upon which
13 applicant relies (i.e., the division of blocks *considering the criticality of the locations*
14 *within the data to be encrypted*) are not recited in the rejected claim(s). Although the
15 claims are interpreted in light of the specification, limitations from the specification are
16 not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed.
17 Cir. 1993).

18

19 (iv) *Furthermore, the notion of arming would be considered inoperable or at least*
20 *impractical in the context of cipher block encryption by a person having ordinary skill in*
21 *the art.* (Remarks, pg. 9)

22

1 Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount
2 to a general allegation that the claims define a patentable invention without specifically
3 pointing out how the language of the claims patentably distinguishes them from the
4 references.

5

6 (v) *Regarding the limitation "executing", the guarding module of the prior art, in*
7 *contrast runs constantly in the background while a "mine" or "software procedure" of the*
8 *present invention does not run in the background and is activated when the mine is*
9 *reached during execution of the protected software or content.* (Remarks, pg. 10)

10

11 In response to applicant's argument that the references fail to show certain
12 features of applicant's invention, it is noted that the features upon which applicant relies
13 (i.e., a "mine" or "software procedure" of the present invention does not run in the
14 background and is activated when the mine is reached during execution of the protected
15 software or content) are not recited in the rejected claim(s). Although the claims are
16 interpreted in light of the specification, limitations from the specification are not read into
17 the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

18

19 (vi) *Applicant respectfully traverses Examiner's rejection of claim 26.*

20 *Applicant respectfully traverses Examiner's rejection of claim 23.* (Remarks, pg.
21 12)

22

1 Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount
2 to a general allegation that the claims define a patentable invention without specifically
3 pointing out how the language of the claims patentably distinguishes them from the
4 references.

5

6 * Regarding the applicant's request for the examiner to reconsider declaration
7 under 37 CFR 1.132 filed December 14, 2005, the examiner respectfully directs the
8 applicant's attention to the final Office Action (2/24/06, pg. 10).

9

10 ***Conclusion***

11

12 Claims 18 – 37 are pending.

13

14 The prior art made of record and not relied upon is considered pertinent to
15 applicant's disclosure.

16

17 *See Notice of References Cited.*

18

19 A shortened statutory period for reply to this final action is set to expire THREE
20 MONTHS from the mailing date of this action. In the event a first reply is filed within
21 TWO MONTHS of the mailing date of this final action and the advisory action is not
22 mailed until after the end of the THREE-MONTH shortened statutory period, then the

Art Unit: 2137

1 shortened statutory period will expire on the date the advisory action is mailed, and any
2 extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of
3 the advisory action. In no event, however, will the statutory period for reply expire later
4 than SIX MONTHS from the date of this final action.

5

6 Any inquiry concerning this communication or earlier communications from the
7 examiner should be directed to Jeffery Williams whose telephone number is (571) 272-
8 7965. The examiner can normally be reached on 8:30-5:00.

9 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
10 supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone
11 number for the organization where this application or proceeding is assigned is 571-
12 273-8300.

13 Information regarding the status of an application may be obtained from the
14 Patent Application Information Retrieval (PAIR) system. Status information for
15 published applications may be obtained from either Private PAIR or Public PAIR.
16 Status information for unpublished applications is available through Private PAIR only.
17 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
18 you have questions on access to the Private PAIR system, contact the Electronic
19 Business Center (EBC) at 866-217-9197 (toll-free).

20

21 Jeffery Williams
22 AU: 2137

23 JW

Jeffrey Williams
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

24